New Enhanced Techniques for Security in Cloud Computing

A Ph.D. Proposal

Submitted to

Swami Ramanand Teerth Marathwade University, Nanded, India

For the degree of

Doctor of philosophy in computer

Under

Faculty of Science and Technology

By

Fursan Mohammed Ahmed Thabit

Under the guidance of

Dr. Sudhir Jagtap

Research Supervisor

Dept . Computer sciences

Data 03/03/2017

Abstract

Cloud computing has a lot of security issues that are gaining great attention nowadays, including the data protection, network security, virtualization security, application integrity, and identity management. Data protection is one of the most important security issues, because organizations won't transfer its data to remote machines if there is no guaranteed data protection from the cloud service providers. Many techniques are suggested for data protection in cloud computing, but there are still a lot of challenges in this subject. The most popular security techniques include SSL (Secure Socket Layer) Encryption, Intrusion Detection System; Multi Tenancy based Access Control, etc. Goal of this paper is to analyze and evaluate the most important security techniques for data protection in cloud computing. Furthermore, security techniques for data protection will be recommended in order to have improved security in cloud computing.

Keywords: access control, authentication, authorization, cloud computing, confidentiality, data protection

.

Table of Contents

Abstract 2
Table of Contents 3
Table of Tables 3
Table of Figures 3
1. Introduction ..... **Error! Bookmark not defined.**
2. Literature Review 5
3. Problem statement: 9
3.1 Problem Specification and Explanation ..... **Error! Bookmark not defined.**
4. Objectives ..... **Error! Bookmark not defined.**
5. The proposed model 10
6. Methodology ..... **Error! Bookmark not defined.**
7. Time plan 11
8. Keywords and abbreviations: 11
References and Bibliography 12

Table of Tables

Table 1: Time Schedule 11

Table of Figures

Figure 1: The proposed model ..... **Error! Bookmark not defined.**

1. Introduction

Cloud computing includes a group of computers that are jointly used to provide different computations and tasks. Cloud computing is one of the most important IT paradigms in the last few years. One of the key benefits that is offered from this IT technology for the companies is reduced time and costs on the market. Cloud computing is providing companies and organizations to use shared storage and computing resources. It is better than to develop and operate with the own infrastructure. Cloud computing also provides organizations and companies to have a flexible, secure, and cost-effective IT infrastructure. It can be compared with the national electric grids that permit organizations and homes to plug into a centrally managed, efficient and cost-effective energy source. Main corporations including Google, Amazon, Cisco, IBM, Sun, Dell, Intel, HP, Oracle, and Novell have invested in cloud computing and propose a range of cloud-based solutions to individuals and businesses.

There are different types and models in cloud computing regarding the different provided services. So, the cloud computing involve public cloud, private cloud, hybrid cloud, and community cloud. Service delivery models, on the other hand, could be categorized as SaaS (Software as a service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). Cloud computing could be usually classified by two ways: by cloud computing location, and by the offered types of services. By the location of the cloud, cloud computing is typically classified in: public cloud (where the computing infrastructure is hosted by the cloud vendor); private cloud (where the computing infrastructure is assigned to a specific organization and not shared with other organizations); hybrid cloud (the usage of private and public clouds together); and community cloud (it involves sharing of IT infrastructure in between organizations of the same community) [1]. If the classification is based on type of offered services, clouds are classified in these ways: IaaS (Infrastructure as a service), PaaS (Platform as a Service), and Software as a Service (SaaS) [1].

Cloud computing as a novel technology for processing and transferring data electronically is nowadays used in almost every computer system. It runs on a network infrastructure that is opened for different types of attacks. DDoS (Distributed Denial of Service) is one of the most known attacks that are used. Syn cookies as well as limitation of the users that are connected with the cloud technology to the server could be used as measures for stopping Distributed Denial of Service.

Other type of attack on the cloud computing technology is man in the middle attack. Secure Socket Layer (SSL) is security technique to overcome this kind of attack. So, if this security technique is not configured properly, authentication of the client and the server might not perform as it should to protect the users of the cloud technology from man in the middle. So, security challenges of data protection when using cloud

computing must be appropriately solved and minimized. When we utilize cloud computing we run our software on hard disks and CPUs that are not in front of us. That is why users are having more doubts about the security issues when they are using this technology. So, a lot of different types of attacks could happen in the cloud technology. Besides the above mentioned, most known attacks involve phishing, IP spoofing, message modification, traffic analysis, IP ports, etc. There are a lot of security techniques for data protection that are accepted from the cloud computing providers, and they all provide authentication, confidentiality, access control and authorization.

2. Literature Review :

The cloud computing platform facilitates huge amount of shared resources to various organizations all over the world on the Internet.

Shen et al. [1] analyzed requirement of security services in cloud computing. The authors proposed a solution for cloud services and build a model of cloud on trust based platform. This model integrate the cloud services for trusted computing platform TCP and trusted platform support services TSS whose basis is on trust component/module. In the last few years, it had emerged and evolved so quickly due to its number of facilities and advantages to the organizations and end users. Many data security factors have also increased due to this fast evolution of cloud in the IT industry. Therefore several security models and trust establishing techniques have been deployed and are been in execution for providing more & more security to the data, especially the sensitive & private one. Despite of that much security, many of the models/techniques lacks in one or more security threat measures.

Neisse et al. [2] have focused on a system of cloud computing that permits review and requirement focused reliability dimensions and distant vital points of attestation for cloud organizations. They build a system that should be applied for Ven platform of cloud computing and also guaranteed trusted technologies that provides security. This system analysis the various related scenarios of different attacks to evaluate that computing in cloud is created on trust. The infrastructures of cloud normally necessitate that stake holders transfers data into cloud based on trust. The frame work that the authors presented in this research has various benefits. According to the scalability and economic point of view, this model provides extra services for cloud computing on trust base. The model is based on various layers. These are cloud computing model, design, security performance and implementation. Xen platform is used for cloud model.

The design of this framework shows the working functionalities of physical hosting service on narrow level and shows history for storage. In this implemented model the author has used some techniques which include integrity management engine, attestation configuration, tamper detection and trusted boot. This model is fully secured and trusted. This model guarantees the security of all kinds of data in form of folder,

reports and fields. System should not be overloaded when DoS command attack occur. In this research, the authors present a solution for malicious problems for cloud customers. He also monitors integrity of files and data on Xen cloud platform. Data's safety, privacy and trust in cloud environment is the main point for its broader adoption.

Yeluriet al. [4]have focused on cloud services according to the security point of view and explore the major challenges of security in cloud at deploying the services. In this research, the authors discussed software vendor and hardware related security issues to enhance the control on cloud services. The authors used a case study of Intel TXT hardware platform for the verification of secure and trusted cloud computing services. They proposed a solution for cloud computing security and for hardware root of trusted computing chain. The methodology that is used for cloud secure is based on the main general three services of the cloud. Authors elaborated following key points and drivers for cloud security, which are identity management, data recovery and management, security in cloud confidentiality, trust, visibility, and assurance and application architecture. They used trusted computing chain that protects cloud data from un-trusted software. Also prevented from unsafe virtual machines, the propose solution for hardware used trusted computer pools and remote attestation. The model proposed by the authors in ensure the security of cloud computing and its services to build a trust.

Behl [5] focused on main security encounters in cloud architecture and environment and had discussed methodologies to cover drawbacks of security problems in cloud architecture and environment. Overall picture of grid computing has been changed by cloud computing. Distribution of data is a new way of cloud computing. In this research, the author proposed a solution for cloud security, complex distributed computing, security strategy, security concerns, and drawback of security challenges. The challenges discussed by the author are insider threats, data loss, service disruption, outside malicious attacks and multi-tenancy issues. There are various challenges for cloud security, but the author proposed a solution for protecting these issues for cloud computing. This research develops comprehensive strategy to face the challenges in cloud security.

Chen et al. [6] has focused on analysis of confidentiality and data sensitivity & security problems in cloud architecture and environment covering all the stages of life cycle of data. In this study, the authors elaborated privacy protection, data security, data segregation, cloud security and cloud computing. They have analyzed these issues and also provided a solution for resolving these issues. These issues are primarily at SPI (SaaS, PaaS, IaaS) level and the major challenge is data sharing. After the analysis of data security and privacy the comprehensive solution is to meet the need of identification and isolation of data is primary task ate design level of cloud based applications.

Cloud computing [7] provide us a podium to use a wide range of services that are based on the internet to deal with our industry procedures & various services of Information technology. But besides its all advantages it also increase the threat for security when a TTP (Trusted Third Party) is involved. By involving a TTP (Trusted Third Party) there is still a chance of heterogeneity of Users which effects security on a cloud. In this research, the authors propose a TTP (Trusted Third Party) independent approach for IDM (Identity Management) with the capability of using unique data on unreliable Data Protection Techniques for Building Trust in Cloud Computing. Using predicate data over the encoded data and using multi organization calculation and computing and active bundle scheme are the approaches used here. In this scheme the bundle has self-reliability checking procedure, it include PII, protection mechanism, privacy policies and virtual machine for policy enforcement of these policies. The resolution lets the use of IDM solicitation on unreliable clouds. Cloud computing is very effective security service that is based on conceptual technology. Data retrieval and safety of the security of data is the main issue in cloud architecture and environment.

Kulkarni et al. [8] have focused on secured cloud services and protection of data by using encryption and decryption techniques at services level. In this research, the authors have highlighted the security threats for cloud computing and also explained techniques to avoid from these threats. In the last few years, it had emerged and evolved so quickly due to its number of facilities and advantages to the organizations and end users. Many data security factors have also increased due to this fast evolution of cloud in the IT industry. Therefore several security models and trust establishing techniques have been deployed and are been in execution for providing more & more security to the data, especially the sensitive & private one. Despite of that much security, many of the models/techniques lacks in one or more security threat measures. In this paper a new model have been designed & proposed which introduces “Security Aware Cloud”. First the trust of the user or organization is established successfully on cloud than the security to the data is granted through privacy and encryption module. Level of quality of service and security are achieved under the Contract Trust layer while the Authentication and Key Management are covered under Internal Trust layer. For critical data privacy and encryption, Homomorphism mechanism is used. Cloud data runs on a network and due to the fact it creates a chance to attack on it. To avoid cloud data from threats the authors proposed the following protection mechanism. Access management and identity features should be authorized, protect server and networks, data storage security, security as a service, security of browser, authentication of users and lock in and data leaking.

Shuanglin [9] have focused on management policy for data security in cloud computing. The authors elaborated management policy and ensure that the internal data needs strong authentication and sensitive information must be filtered. Cloud is an internet bases service and all the data is on networks. In this research, the authors design a policy for data protection of cloud clients. When data is on public cloud then

protection of data is complex issue. The policy that the authors design based on following methods. These are: Authentication technology, Visualization of Sensitive data, and technical support sections, filtration of sensitive data, establish safe management system, cloud computing gateway and classification of data evaluation.

Squicciarini [10] has focused on problems disclosure and damage to the sensitivity of data's privacy in cloud computing. Cloud computing provides a highly sensitive services on internet to individuals or large organizations. User worry about the leakage of data and loss of privacy in cloud service. In this research, the authors proposed a three tier solution to prevent from data leakage and privacy loss. These tiers are: lower protection, medium protection and strong protection. According to the researcher the strong protection tier prevents sensitive data of user profile from service provider. Medium level tier prevents from indexing effectiveness. The last protection tier forces user to obey the policy of cloud data. The authors proposed a new technique for the prevention of data leakage and loss of privacy and this technique is helping toward the seven tier protection techniques. Cloud computing provides a new business services that is based on demand. The cloud networks have been built through dynamic virtualization of hardware, software and datasets.

Hwang and Li [11] focused on trust in cloud computing on the basis of secure services. The authors explained the protection procedures to build trust in cloud computing. They discussed about cloud platforms, cloud service provider and security features for these services. They proposed a reputation management trust model that defined the different areas which were based on the different phases of cloud computing. Data coloring mechanism and secure data access mechanism is discussed by the authors in this paper and used the same mechanism for their framework. Cloud security infrastructure and the trust reputation management play a vital role to upgrading the cloud services.

Iqbal et al. [13, 14] proposed performance metrics for software design and software project management. Process improvement methodologies are elaborated in [15, 16] Khan et al. [17] carried out quality assurance assessment.

Amir et al. [18] discussed agile software development processes.

Khan et al. [19] and Khan et al. [20] analyzed issues pertaining to database query optimization and requirement engineering processes respectively.

Umar and Khan [21, 22] analyzed non-functional requirements for software maintainability. Khan et al. [23, 24] proposed a machine learning approaches for post-event timeline reconstruction. Khan [25] suggests that Bayesian techniques are more promising than other conventional machine learning techniques for timeline reconstruction. Rafique and Khan [26] explored various methods, practices and tools being used for static and live digital forensics.

In [27], Bashir and Khan discuss triaging methodologies being used for live digital forensic analysis. References [28-44] reviewed different techniques in different domains and reported their critical evaluations along with a workable framework where necessary.

3. Problem statement:

Two main challenges of cloud computing are security, integrity and reliability . Clients' needs guarantee that their data which is stored on cloud will not be accessed by other clients. To achieve security on cloud there are so many techniques and algorithm available. Some of these techniques are:

Encryption: In this technique complex algorithm are used to hide the original information with the help of encryption key. The data is converted into unreadable form called cipher text and then stored on remote server storage.

Authentication processes: In this process, a login mechanism is used to verify that the only authenticated user is accessing the cloud data. It requires creating a user name and password.

Authorization practices: A list of Authorized client is used to identify, who can access data stored on cloud system.

However, many people still worry that data saved on a remote storage system could be accessed by other clients and they will alter it. . Hackers could also attempt to steal the physical machines on which data are stored. An employee from cloud service provider could alter or destroy data using his or her authenticated user name and password. Instead of all these risks, clients are adopting cloud computing widely. Cloud storage companies are investing a lot of money to make sure that their clients data would be safe. They are trying to limit the possibility of data theft or corruption.

We are discussing some techniques here that are helping how to get security on cloud .

4. Objectives:

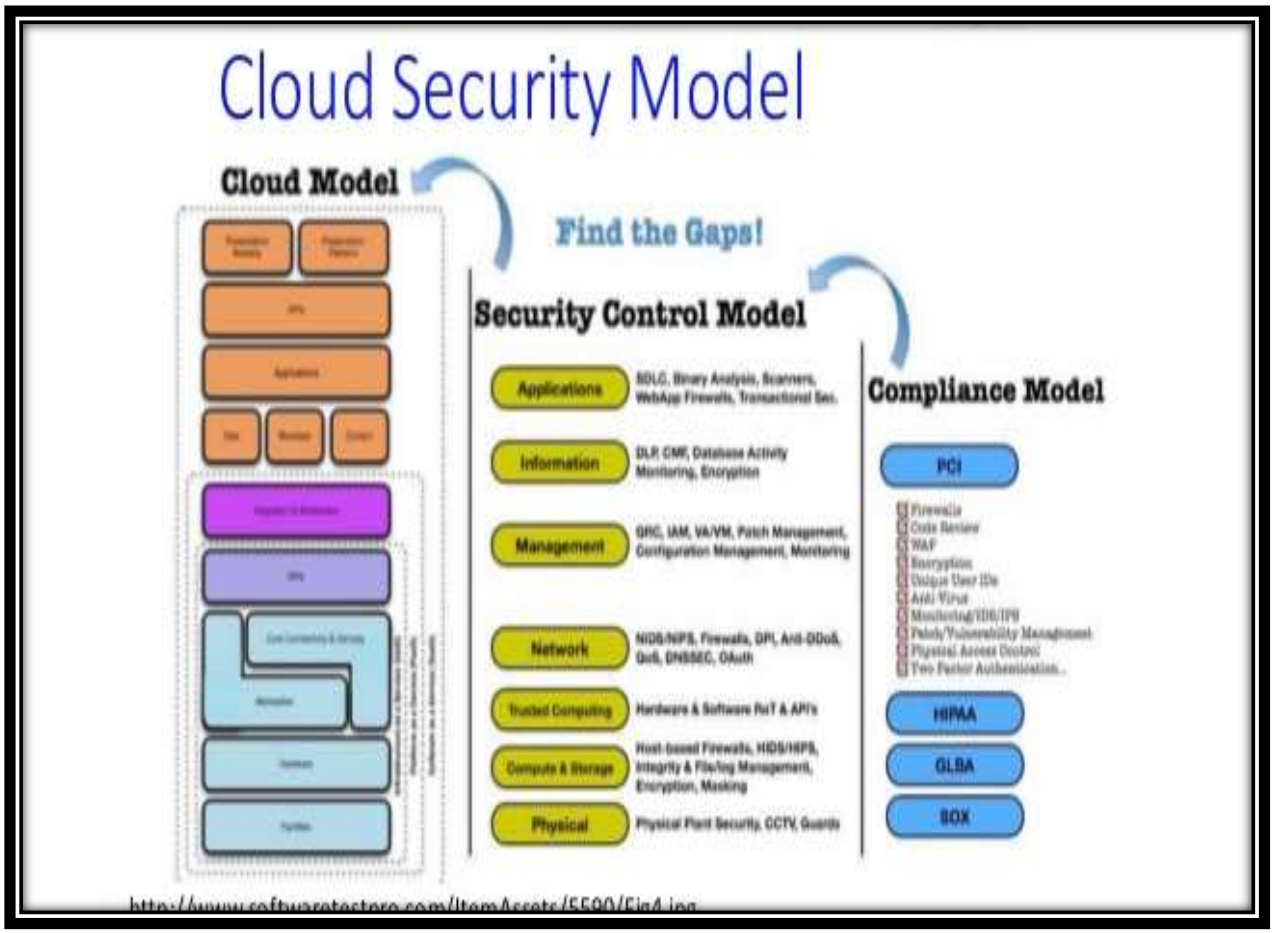
Main:

We aim to study the cloud computing security techniques and we will work to new enhanced techniques for security in cloud computing.

- To study the techniques approaches for cloud computing security of over network in Cloud using proper authentication, , integrity and confidentiality.
- To enhanced techniques which securely cloud computing over network and provides three way protection in terms of authenticity, integrity and confidentiality
- To achieve confidentiality and integrity of the data.
- To verify and validate the proposed

5. The proposed model:

In this section, a new enhanced for protecting data in cloud computing environments using the information stated in the previous section is offered. We aim to study the cloud computing security techniques and we will work to new enhanced techniques for security in cloud computing.



6. Methodology

We aim to new enhanced techniques for security in cloud computing. First, we will study the literature and the real techniques are used for security cloud computing . This will be according to a study for many previous related works with cloud computing security in every possible field (authenticity, integrity and confidentiality). Then will suggest which technique of the cloud which we will work on it , we will suggest the needed standards and circumstances adopt the resulted model in order to have a cloud computing security . The final step will be to develop a sample example for the model and to test it to prove that it is applicable.

Statistically, we will make some questionnaire which will target the students and employees in the ministry and its institutions and the banks. We will visit some institutions to have a real observation every time according to the allowance from the management. Then empirically we will develop the new enhanced techniques in c cloud computing security and will test it with a sample dataset with the agreement of one or two institutions in India. The final results after that can be generalized

7.Time plan

Table 1: Time Schedule

Stage of the dissertation writing process	Number of weeks needed	Start date	End date
STAGE ONE: Reading and research			
a) Seek to identify an original, manageable topic	2	1/12/2016	14/12/2016
b) Reading and research into chosen topic	3	15/12/2016	5/1/2017
STAGE TWO: The detailed plan			
a) Construct a detailed plan of the dissertation	3	6/1/2017	26/1/2017
STAGE THREE: Initial writing			
a) Draft the various sections of the dissertation	12	27/1/2017	18/4/2017
b) Undertake additional research where necessary	6	19/4/2017	8/6/2017
STAGE FOUR: The first draft			
a) Compile and collate sections into first draft of dissertation	30	9/6/2017	5/3/2018
b) check the flow of the dissertation	6	6/3/2018	17/4/2018
c) Check the length of the dissertation	3	18/4/2018	15/5/2018
d) Undertake any additional editing and research	3	16/5/2018	12/6/2018
STAGE FIVE: Final draft			
a) Check for errors	25	13/6/2018	7/12/2108
b) Prepare for submission	6	8/12/2018	19/1/2019
c) Final proof-read (by a friend or yourself) and final editing	12	20/1/2019	12/4/2019
d) Compile bibliography	4	13/4/2019	11/5/2019
e) Get the dissertation bound	5	12/5/2019	16/6/2019
f) Submit your dissertation	15	17/6/2019	2/10/2019

1. Keywords and abbreviations:

- **Cloud Computing security :** is a transformative approach as it promises much more than a data center model. It fundamentally changes how we interact with information. The cloud provides services on demand at the infrastructure, platform, or software level [15].
- **On-demand services:** are the services which are provided according to the needing of the end-user [15].
- **Scalable infrastructure:** means providing hardware resources according to the load balancing [15].
- **Churn-Resilient Protocol (CRP):** A solution to increase fault tolerance in proximity-aware overlays is to guarantee connectivity of critical links, such as random links among clusters or nodes [15],

References and Bibliography

[1] Ling Qian, Zhiguo Luo, Yujian Du and Leitao Guo, “Cloud Computing: An Overview”, Springer-Verlag Berlin Heidelberg CloudCom,
LNCS 5931, pp. 626-631, 2009.
[2] Peter Mell and Timothy Grance, “The NIST Definition of Cloud Computing”, National Institute of Standards and Technology Special
Publication 800-145, 2011.
[3] Tharam Dillon, Chen Wu and Elizabeth Chang, "Cloud Computing: Issues and Challenges", 24th IEEE International Conference on
Advanced Information Networking and Applications, pp. 27-33, 2010.
[4] S. Ramgovind, MM. Eloff and E. Smith, “The Management of Security in Cloud Computing,” IEEE Information Security for South
Africa (ISSA), pp. 1-7, 2010.
[5] Sherif el-etriby, Eman M. Mohamed and Hatem S. Abdelkader, “Modern Encryption Techniques for Cloud Computing Randomness and
Performance Testing,” 3rd International Conference on Communications and Information Technology (ICCIT), pp. 800-805, 2012.
[6] Satish Kumar and Anita Ganpati, “Multi-Authentication for Cloud Security: A Framework," International Journal of Computer
Science & Engineering Technology (IJCSET),Vol. 5, Issue 4, pp. 295-303, Apr. 2014.
[7] V. Sulochana and R. Parimelazhagan, “A Puzzle Based Authentication Scheme for Cloud Computing,” International Journal of
Computer Trends and Technology (IJCTT), Vol. 6, Issue 4, pp. 210-213, Dec. 2013.
[8] Prashant Rewagad and Yogita Pawar, “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to
Enhance Data Security in Cloud Computing,” IEEE International Conference on Communication Systems and Network Technologies
(CSNT), pp. 437-439, 2013.
[9] Sarbjeet Singh and Maninder Singh, “Design and Implementation of Multi-tier Authentication Scheme in Cloud," International
Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 5, pp. 181-187, Sep. 2012.
[10] H.A. Dinesha and V.K. Agrawal, “Multi-level Authentication Technique for Accessing Cloud Services," IEEE International Conference
on Computing, Communication and Applications (ICCCA), pp. 1-4, 2012.
[11] Neha Tirthani and R. Ganeshan, “Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography,"
International Association for Cryptologic Research (IACR), ePrint archive, 2014.
[12] Eman M. Mohamed, Hatem S. Abdelkader and Sherif el-etriby, “Enhanced Data Security Model for Cloud Computing,” IEEE 8th
International Conference on Informatics and Systems (INFOS2012), pp. CC12-CC17 , 2012.
[13] Uma Somani, Kanika Lakhani and Manish Mundra, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the
Data Security of Cloud in Cloud Computing”, IEEE 1st International Conference on Parallel, Distributed and Grid Computing
(PDGC2010), pp. 211-216, 2010
[13]. B. Nedelcu, et al. “Cloud Computing and its Challenges and Benefits in the Bank System”, Database Systems Journal, 4(1), 2015.

.[14] K. Chandrasekaran. “Essentials of cloud computing”. CRC Press, 2014.

.[15] T. Dillon, C. Wu, and E. Chang. “Cloud computing: issues and challenges”. 24th IEEE international conference on advanced information networking and applications, IEEE, 2010, pp:27-33.

.[16] K. Hwang, J. Dongarra, and G. C. Fox. “Distributed and cloud computing: from parallel processing to the internet of things”. Morgan Kaufmann .2013 .

.[17] T. M. Mbelli, and B. Dwolatzky. “Cyber Security, a Threat to Cyber Banking in South Africa: An Approach to Network and Application Security”. Cyber Security and Cloud Computing (CSCloud), 2016 IEEE 3rd International Conference, IEEE, 2016, pp. 1-6.

.[18] A. Brown, “How the cloud will reshape transaction banking”, Building tomorrow, 2014.

.[19] I. Mohammed AM. "Exploring the Feasibility of Adopting Cloud Computing in Computer Center Taiz University." International Journal of Advanced Networking and Applications 6.4 (2015): 2359.

.[20] M. M. Alabbadi. "Cloud computing for education and learning: Education and learning as a service (ELaaS)." Interactive Collaborative Learning (ICL), 2011 14th International Conference on. IEEE, 2011.

.[21] I. Ewuzie, and A. Usoro. "Exploration of cloud computing adoption for e-learning in higher education." Network Cloud Computing and Applications (NCCA), 2012 Second Symposium on. IEEE, 2012.

.[22] A. A. S. Sunday, and E. Y. A. P. EkeB. "Cloud Computing: A Catalyst in the Agenda of Education for all (EFA".(

[23]. NAGASURENDRAN, P. "Cloud Computing–Present Trends in Education." International Journal of Scientific Research 5.9 (2017).

The Researcher / Student **The Research Guide**

Fursan Mohammed Ahmed **Dr. Sudhir Jagtap**